

Discrete Parts Manufacturing - Requirements Identification

1. Control System Access Control

Discussion: System device access was discussed in the context of the human user. The distributed and autonomous nature of control systems and their devices requires that device access be addressed in terms of component-to-component access in the absence of human intervention.

Essential Issue: Who can do what, where, and under what circumstances (role dependent, system state dependent).

Implications: It is insufficient to say – “we want role-based access control” without going the next step of characterizing the types of roles and types of accesses. It need not be detailed but it must be more than “give me access control”. Where are the access control rules to be applied?

State-based access control

Discussion: As a subset of the access control mechanism discussion the idea of incorporating systems or process state into the access control decision was presented. This discussion illustrates why it is insufficient to state access control requirements in terms abstract statements, and illustrates one way in which an access control capability can be tailored to address control system specific issues. State information (the state of the machine, the state of the process) plus who you are, where are you, what role do you have, what are you trying to do, what have you done) are all factored into the decision to grant/deny an access or operation request.

Essential Issue: Allowing the policy enforcement mechanism to be aware of state information.

Implications: The needs and capabilities of the various process industries are likely to differ in this context. This is a good discussion topic since the first step is to determine if such a need is credible for a particular industry.

Time and Location Sensitive Access control rules

Discussion: Discussion regarding unscheduled access by an individual to the system illustrated the need for a wider scope policy to not just establish roles and access rights but to also define access in terms of location and time of day.

A full scope addressing of this issue would also include component-to-component access rules to prevent automated access by a device outside the bounds of defined normal access times or mechanisms.

Loss of remote access as a security precaution can have a negative impact

Discussion: This discussion focused on technology use policy and the implications of such policy. The issue was that instituting a “no remote access” policy would affect efficient operation of the control system. The issue is subjective since the impact is not general; it is specific to the way a particular organization has chosen to do business. More importantly, the issue brings to light the fact that a policy decision may require a complete re-think of business operations. In terms of the requirements spec, the issue is meaningful only after a decision has been made and then, how the system might be used to enforce the policy.

2. Communications Integrity

Discussion: Although the focus was on wireless, the bottom line is there must be security over the accessible communications channels.

Essential Issue: Wireless is the medium – so effectively the issue is a specific form of networking – not about a new capability.

Implications: Unless and until specific vulnerabilities of wireless mediums are determined to be significantly different than that of wired mediums, there is nothing different in the way the general requirements for networked information flow, integrity and authentication etc. are specified.

3. Control System Integrity

Security of audit function and data

Discussion: These are the standard issues of ensuring the protection of the functions and data associated with maintaining event logs and audit trails. Other than the issue of what does audit mean in a control system context (i.e., what type of activity and what types of events are recorded) there were no unique issues brought up. This issue is closely related to the CIDS issue since the detection capability might utilize event traces as a means to detect potential policy violations.

4. Intrusion Detection and Response

Discussion: The discussion was initiated in response to the statement that there is a need for proactive response to an attack. Proactive response to an attack is considered as meaning automatic response to an attack, that is, without human intervention. Discussion of intrusion detection system (IDS) capabilities often occurs in the absence of a statement of the norm; an IDS needs to know what is normal to detect the abnormal.

Another frequent misconception in terms of IDS application is its use as a “policy enforcement mechanism” to catch violators of system use policies (e.g., if I have legitimate access to the system and legitimately install software and that software does something bad to my system – I cannot expect the IDS to detect the behavior and respond to it).

Essential Issue: What is intrusion detection? In the absence of a contextual base the phrase is meaningless.

Implications: Incident response requires that there is first incident detection. The detection capability may be fully or partially automated.

Intrusion detection at control network level (Control IDS)

Discussion: The need for capabilities to monitor activity on the control network and to detect activity that is beyond 'nominal' was discussed (i.e. Control IDS). The issues with this need is 'nominal' must be defined. By defining the norm a policy may then be established and only then will it be possible to detect potential violations of policy (i.e., an intrusion). The next step would be to define policy for the response to the potential intrusion.

There are then two lower-level issues:

1. within what constraints is the detection component to operate. The detection process will consume bandwidth and cycles – so how much budget will be allocated to such processes?
2. what type of response capabilities are desired? There is this overwhelming notion that the process does not stop – so, what effective response can be had with a process control system should a “potential” violation be detected? The issue is that of response to a potential false alarm. Significant trust in the accuracy and validity of the control IDS is necessary.

5. Operational Assurance Maintenance

Runtime Configuration Management

Discussion: The problems of runtime configuration management were discussed from the perspective of having and enforcing a policy as opposed to defining specific runtime CM needs and capabilities. The term used was to have a “SLAM Proof” system – and the meaning behind the phrase is push capability for software updates and the need is for the capability to disable the authorization to invoke the function.

Essential Issue: Configuration control in the runtime environment has the aspects of restricting the ability to modify the installed baseline, determining the installed base and verifying correctness of the installed base.

Implications: There must be policy established to work in conjunction with the runtime capabilities built into the system.

6. Evolutionary Assurance Maintenance

Discussion: The issue was presented as commodity hardware and software security inheritance. The issues are several:

1. how do you ensure that as individual products mature from version to version that equivalent security functionality is maintained and that when these products are integrated into the control system that equivalent security functionality is provided
2. how do you ensure that as individual products mature from version to version that equivalent security functionality is maintained and that when these products are integrated into the control system that equivalent assurance is achieved
3. how often do you reassess the environment, technology, personnel and operational policies to adjust to changes in any/all of the environment, technology, personnel and operational processes
4. to what extent do you re-validate the security posture after a component changes

Migration strategies for system retrofit

Discussion: The issue is the process followed to take a system from a given operational state to some other operational state. Several implications are found in this statement:

1. The current and new state must be known and defined
2. The process must incorporate both computer and personnel aspects
3. Checks-n-balances must be instituted where appropriate to ensure that the process is being executed properly, to verify that the process is accurately defined and to make adjustments in the process where necessary.

This issue has the two key components:

1. determining that the migration to a new system is necessary (outside the scope of stating security criteria but related to the criteria since the decision to go/no go may factor in cost of a specific migration)
2. defining the process of then doing the requirements engineering (amongst other things) within the bounds established by the process

Obsolescence and backwards compatibility

Discussion: The issue is determining what must be done to ensure continued interoperability with existing components of a control system implementation as new components are acquired and installed as either replacements or extensions.

Global differences in security requirements must be comprehended

Discussion: Security systems as well as any other system that interfaces with the control system must not impact control performance. The security mechanisms must be implemented within existing functional, performance and safety constraints.

This issue is more a statement of governing principle and must be refined to specifically state constraints and the security processing capability in the context of the identified constraints.

7. Operating Policy Analysis, Definition, Enforcement

Business Continuity

Discussion: This issue was presented as disaster recovery. The issues of knowing what can happen, what the implications are if something should happen, and what to do when it happens. These issues are largely outside the scope of detailed security criteria (other than fail-secure, automatic recovery) and are also largely non-IT procedural issues. The connection to the security criteria is in the need for total system certification testing which would include the verification of any mechanisms of the control system that support the business continuity policy

Regulatory concerns – 21 CFR Part 11

Discussion: The issue of ensuring compliance with regulatory mandates requires identification of such mandates and the assessment of how to incorporate the appropriate language in the requirements spec to ensure that such compliance may be demonstrated. Specifically, issues governing electronic information, signatures, etc. exist.

More information is required to understand the scope and context of such regulatory material.

Risk assessment for production environment

Discussion: The issue is that such an activity must be done on a periodic basis and the results utilized throughout the system development and operational life-cycles.

Security system validation

Discussion: The issue is what must be done to determine that the solutions being sought actually serve to solve the problem. This is not a specification development issue – this is an issue regarding the establishment of a strategy within which one such activity is the development, validation and verification of the specification.

Migration strategies for system retrofit

Discussion: The issue is the process followed to take a system from a given operational state to some other operational state. Several implications are found in this statement:

1. The current and new state must be known and defined
2. The process must incorporate both computer and personnel aspects
3. Checks-n-balances must be instituted where appropriate to ensure that the process is being executed properly, to verify that the process is accurately defined and to make adjustments in the process where necessary.

This issue has the two key components:

3. determining that the migration to a new system is necessary (outside the scope of stating security criteria but related to the criteria since the decision to go/no go may factor in cost of a specific migration)
4. defining the process of then doing the requirements engineering (amongst other things) within the bounds established by the process

Benefits of security – insurance, other fiduciary

Discussion: The discussion focused on who is the beneficiary of instituting effective security measures and what organizations might have a role to influence more widespread application of effective security measures. The context of this statement was more to convince management that security is good and necessary rather than the direct benefit or relationship to the efforts to effect security in control systems.

Cost of security

Discussion: The issue is how much will the security cost and who is going to pay for it. This issue is not directly related to the development of criteria, it is more associated with the bounds within which security will be implemented (total cost) or the determination of cost/benefit of a proposed solution.

8. Collaborative Working Relationships

Discussion: This issue was presented in the context of vendor liability. The ensuing discussion focused on the need for well-defined rules for interaction with business partners and the need for ramifications that are enforced should the rules be violated. The discussion touched on policy for collaboration agreements (ISAs, MOUs) and included security training and awareness, and philosophies on distributed vice centralized access arrangements.

Essential Issue: Establishment of business rules for interactions with customers and vendors. This is not an IT issue (strictly policy), however, the rules established must be verified as being implemented as defined.

Implications: None, unless the policy has aspects that are enforced by the control system.

On-Site Third Party Individuals

Discussion: There is a need for policies and standard operating procedures governing the interactions of on-site third party individuals and the control system personnel and operations. This again is a policy definition/execution issue. Specific issues were not discussed. However, the relationship between this issue and the requirements for the control system is that the control system may be utilized to enforce aspects of the policy that is defined. It is not expected that such requirements go beyond that which would be required to enforce policies over internal control system personnel.

9. Security Ownership

Discussion: In response to the question “Who owns security on the floor” the response was varied and in fact, no one really owns security. This is an organizational and structure issue and has to do with the enforcement of whatever rules are put in place for the secure operation of the control system. Again, a policy issue.

Definition of new roles and responsibilities with authority to make the above happen

Discussion: This was more of a comment made in response to all the policy discussion that there is a need for restructuring management to ensure there exists a single authority with responsibility for all computer operations, and to remove the top-level distinction between control and IT systems.

Question: In what ways can vendors better support the implementation and integration process that precedes going operational with new components/technologies?

Answer: Silence.